Synopsis for Ph.D. Programme

Title: Chaos based cryptography and its application to secure communications

Name of the Candidate: Subhrajit Roy

Name of the Guide: Dr. Amar Prasad Misra

Registration No. : VB-2139 of 2015-16

Date of Registration: 28/07/2015

Keywords: Chaos Theory, Nonlinear Dynamics, Cryptography.

The study of chaotic dynamical systems and their possible applications to Cryptography have received considerable attention over the past many years in scientific community. Chaotic systems are usually characterized by sensitive dependence on initial conditions, similarity to the random behaviors, and continuous broad-band power spectrum. The possibility of self-synchronization of chaotic oscillations has sparked an avalanche of works on application of Chaos in Cryptography. Many fundamental concepts in Chaos theory such as mixing, measure pressuring transfer-motions and sensitivity have been applied for cryptography.

In recent years, a large number of works have been focused on chaos based cryptosystem. There are three main issues- implementation, key management and security analysis. The main implementation of chaos based cryptography is over Data Encryption Standard (DES) or Advanced Encryption Standard (AES). Recent works have been developed over DES using Block ciphers.However, these are made mostly on conventional cryptography which is rather marginal due to two reasons. Firstly, almost all chaos-based cryptographic algorithms use dynamical systems defined on the set of real numbers, and therefore are difficult for practical realization and circuit implementation. Secondly, security and performance of almost all proposed chaos-based methods are not analyzed in terms of the techniques developed in cryptography. Moreover, most of the proposed methods generate cryptographically weak and slow algorithms. We also see that there is a significant connection between Chaos and cryptography. In early 1950, 'Claude Shannon' explicitly mentioned that the basic stretch-and-fold mechanism of chaos can be used in cryptography. He stated that-"*Good mixing transformations are often formed by repeated products of two simple non-commuting operations. Hopf has shown, for example, that pastry dough can be mixed by such a sequence of operations. The dough is first rolled out into a thin slab, then folded over, then rolled, and then folded again, etc.*" There are many similarities between Chaos and Cryptography, like sensitivity to initial conditions in chaos is similar to the key dependent confusion and diffusion, i.e. in Chaos theory small variation of any variable changes the outputs considerably which behavior is similar in Cryptography that modification of 1 bit of the plaintext or key should change all bits of the plaintext with probability 50%. We also see that there are two main approaches of designing Chaos-based Cryptosystem are Analog and Digital. Most analog chaos-based cryptosystems are secure communication schemes designed for noisy channels, it means that two chaotic systems can synchronize with each other under the driving of one or more scalar signals, which are generally sent from one system to another. In chaos-synchronization-based cryptosystems, the information can be transmitted by one or more chaotic signals in a number of ways, such as, chaotic masking, chaotic switching or chaos shift keying (CSK), chaotic modulation, chaos control methods, inverse system approach etc. In this method the receiver has to synchronize with the transmitter's chaotic generator so as to generate the chaotic carrier signal x(t) thereby recovering the message signal m(t) via signal separation. On the other hand

in Digital chaos-based cryptosystems, one or more chaotic maps are implemented in finite computing precision to encrypt the plain-message in a number of ways, such as-Stream ciphers based on chaos-based PRNG (Pseudo Random number generator), Chaotic stream ciphers via inverse system approach, Block ciphers based on chaotic round function or S-boxes, Block ciphers based on forward/backward chaotic iterations, Chaotic ciphers based on searching plain-bits in a chaotic pseudo-random sequence etc. In the all of the above cases these ciphers do not depend on chaos synchronization at all, they usually use one or more chaotic maps in which the initial conditions and the control parameters play the role of the secret key.

The main objective of the work includes the implementation, key management and security analysis of a Chaos based Cryptosystem. We also would like to propose new chaos based secure communication schemes through different nonlinear media such as, semi-conductor laser, Internet, Wireless network etc. using AES or DES algorithm. Here, we introduce chaos in a non-linear dynamical model and generate more secure keys using the chaotic medium. We also plan to implement more time efficient schemes.

References:

[1] Kocarev, L. [2001] "Chaos-based cryptography: A brief overview," IEEE Circuits and Systems Magazine 1,6–21.

[2] Kocarev, L.: Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps. IEEE Transactions on Circuits and Systems I 48, 163-169.

[3] B. Preneel, V. Rijmen, and A. Bosselears,"Recent Developments in the Design of Conventional Cryptographic Algorithms", *Lecture Notes in Computer Science*, vol. 1528, pp. 105–130, Springer -Verlag, Berlin, 1998.

[4] M. S. Baptista, "Cryptography with Chaos", *Physics Letters A*, vol. 240, pp. 50–54, 1998.

[5] G. Jakimoski and L. Kocarev, "Analysis of Some Recently Proposed Chaos-Based Encryption Algorithms", submitted for publication.

[6] C. E. Shannon, "Communication Theory of Secrecy Systems", *The Bell SystemTechnical Journal*, vol. 28, no. 4, pp. 656– 715, October 1949.

[7] C. E. Shannon, "A Mathematical Theory of Communication", *The Bell SystemTechnical Journal*, vol. 27, no. 3, pp. 379– 423, July 1948.

[8] W. Diffie and M. E. Hellman, "New Directions in Cryptography", *IEEE Transactionson Information Theory*, vol. 22, pp. 644–454, 1976.

[9] X. Lai and J. L. Massey, "A Proposal for a New Block Encryption Standard", *Advancesin Cryptology - EUROCRYPT'90*, pp. 389–404, Springer-Verlag, Berlin, 1991.

[10] G. Jakimoski and L. Kocarev, "Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps"

[11] T. Habutsu, Y. Nishio, I. Sasase, and S. Mori, “A secret key cryptosystem by iterating a chaotic map,” in *Proc. Advances in Cryptology—EUROCRYPT’91*. Berlin, Germany: Springer-Verlag, 1991, pp. 127–140.

[12] Z. Kotulski and J. Szczepanski, “Discrete chaotic cryptography,” *Ann. Phys.*, vol. 6, pp. 381–394, 1997

[13] Y. H. Chu and S. Chang, “Dynamical cryptography based on synchronizedchaotic systems,” *Electron. Lett.*, vol. 35, pp. 974–975, 1999.

[14] E. Alvarez, A. Fernandez, P. Garcia, J. Jimenez, and A. Marcano, “New approach to chaotic encryption,” *Phys. Lett. A*, pp. 373–375, 1999.

[15] H. Feistel, “Cryptography and computer privacy,” *Scientific American*, vol. 228, no. 5, pp. 15–33, 1973.

[16] E. Biham and A. Shamir, “Differential cryptanalysis of DES-like cryptosystems,” in *Advances in Cryptology—CRYPTO’90*. Berlin, Germany: Springer-Verlag, 1991, pp. 2–21.

[17] M. Matsui, “Linear cryptanalysis method for DES ciphers,” in *Advances in Cryptology EUROCRYPT’93*. Berlin, Germany: Springer-Verlag,1994, pp. 386–397.

[18] E. Biham and A. Shamir, *Differential Cryptanalysis of Data Encryption Standard*. Berlin, Germany: Springer-Verlag, 1993.

[19] ´Alvarez, E., Fern´andez, A., Garc´ıa, P., Jim´enez, J. &Marcano, A. [1999a] “New approach to chaotic encryption,” Phys. Lett. A 263, 373–375.

[20] Boccaletti, S., Kurths, J., Osipov, G., Valladares, D. & Zhou, C. [2002] “The synchronization of chaotic systems,” Phys. Rep. 366, 1–101.

[21] L. M. Pecora and T. L. Carroll, “Synchronization in Chaotic Systems”, *PhysicalReview Letters*, vol. 64, no. 8, pp. 821–824, 1990